

UNITED STATES DISTRICT COURT

for the
Southern District of OhioFILED
RICHARD W. NAGEL
CLERK OF COURT

9/28/21

In the Matter of the Search of
(Briefly describe the property to be searched
or identify the person by name and address)

Case No. 3:21MJ358

U.S. DISTRICT COURT
SOUTHERN DIST. OHIO
WEST. DIV. DAYTON[REDACTED]
including all curtilage and vehicles**APPLICATION FOR A SEARCH WARRANT BY TELEPHONE OR OTHER RELIABLE
ELECTRONIC MEANS**

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

SEE ATTACHMENT A

located in the Southern District of Ohio, there is now concealed (identify the person or describe the property to be seized):

SEE ATTACHMENT B

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section

Offense Description

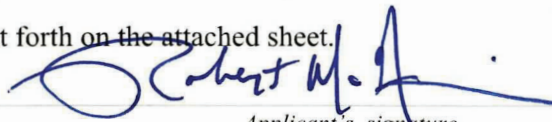
18 U.S.C. § 1343

Wire Fraud

The application is based on these facts:

SEE ATTACHED AFFIDAVIT

- ☒ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.



Applicant's signature

SA ROBERT MCGUIRE, FBI

Printed name and title

Sworn to before me and signed in my presence via facetime.

Date: 9/28/21

City and state: Dayton, Ohio



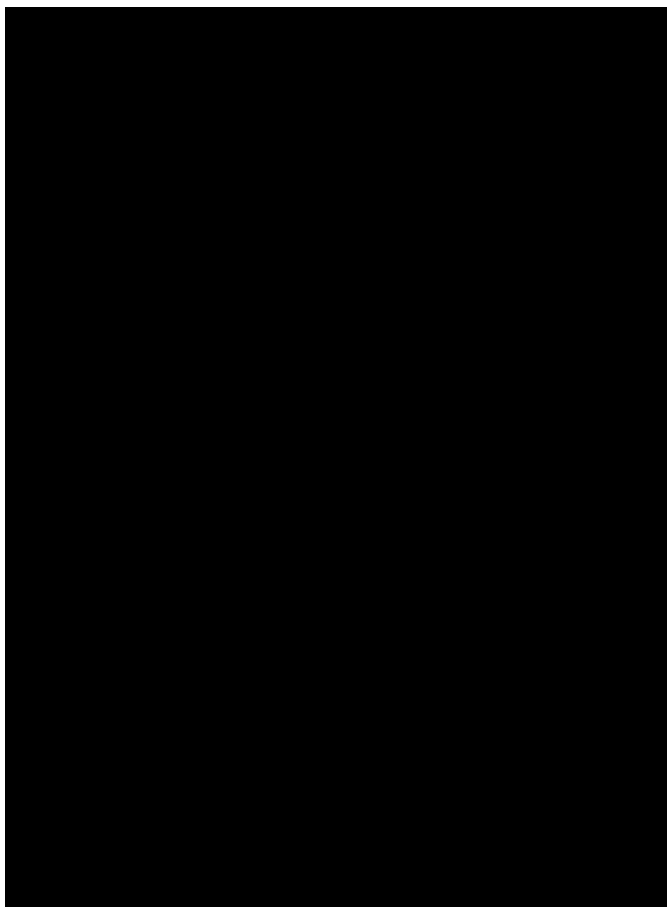
s signature

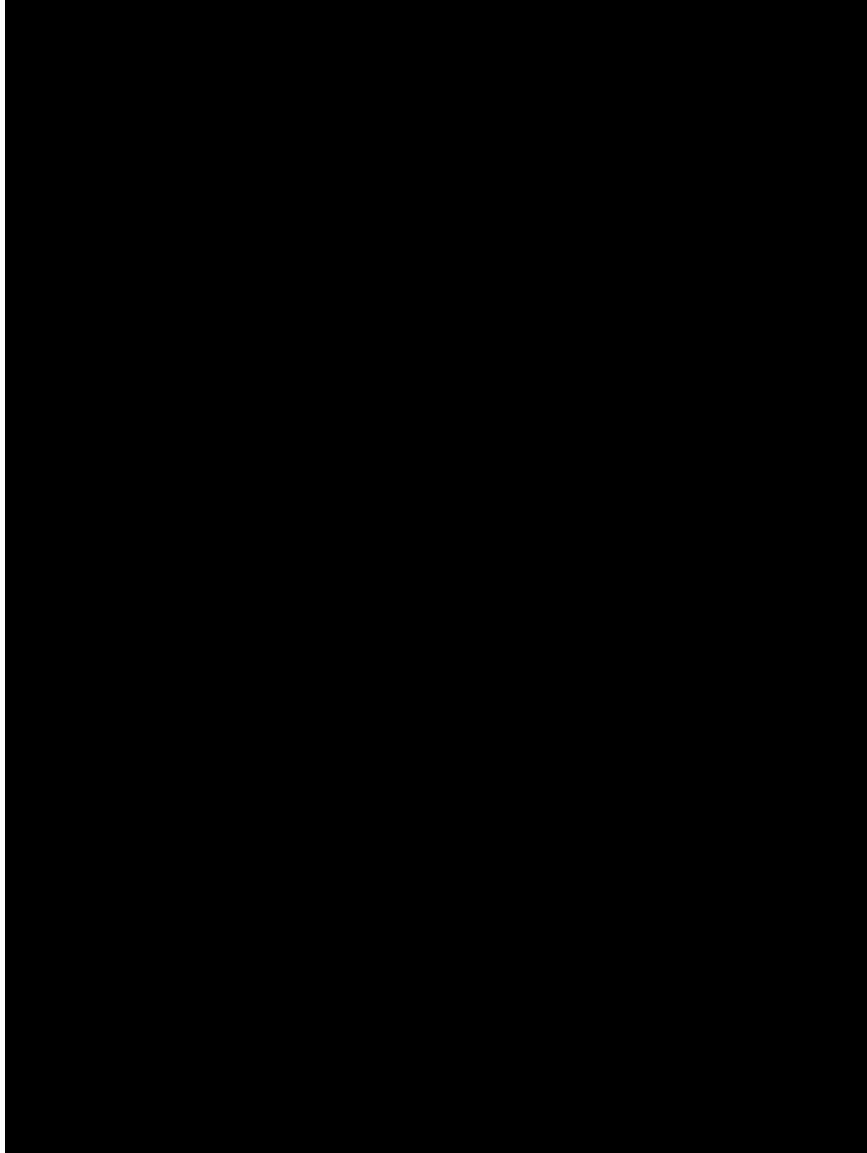
, U. S. Magistrate Court
ame and title

ATTACHMENT A

Property to be searched

The property to be searched is [REDACTED], further described as a small ranch house facing west. The house is brick on the lower half and has siding on the top half. The residence appears dark in color with white trim, including trim surrounding each window. There are three windows on the front of the house and a front door to the south of the southern most of the three windows. Adjacent to the front door is a one car garage, containing the address, [REDACTED] above the white garage door and below the roof of the house. There is a giant star hanging on the front of the house.





ATTACHMENT B

Property to be seized

1. All records containing possible evidence of violations of 18 U.S.C. § 1343 (wire fraud), those violations involving [REDACTED] and possibly others, and occurring after January 1, 2017, including:

- a. Records and information relating to a conspiracy to defraud Individual 1;
- b. Records and information relating to the identity or location of additional suspects and/or victims;
- c. Records relating to transactions involving Bitcoin, rubber, trailers, cars and/or real estate.

2. Any computer, storage medium, and/or cell phones.

3. For any computer, mobile phone, or storage medium whose seizure is otherwise authorized by this warrant, and any computer, mobile phone, or storage medium that contains or in which is stored records or information that is otherwise called for by this warrant (hereinafter, “COMPUTER”):

- a. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, “chat,” instant messaging logs, photographs, and correspondence;

- b. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;
- c. evidence of the lack of such malicious software;
- d. evidence indicating how and when the computer was accessed or used to determine the chronological context of computer access, use, and events relating to crime under investigation and to the computer user;
- e. evidence indicating the computer user's state of mind as it relates to the crime under investigation;
- f. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;
- g. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER;
- h. evidence of the times the COMPUTER was used;
- i. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;
- j. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;
- k. records of or information about Internet Protocol addresses used by the COMPUTER;

- l. records of or information about the COMPUTER's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses;
- m. contextual information necessary to understand the evidence described in this attachment.

As used above, the terms "records" and "information" includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

The term "computer" includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

The term "storage medium" includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

This warrant authorizes a review of electronic storage media and electronically stored information seized or copied pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law

enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the seized or copied electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

4. Routers, modems, and network equipment used to connect computers to the Internet.

As used above, the terms “records” and “information” includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

The term “computer” includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

The term “storage medium” includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

This warrant authorizes a review of electronic storage media and electronically stored information seized or copied pursuant to this warrant in order to locate evidence, fruits, and

instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the seized or copied electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

IN THE UNITED STATES DISTRICT COURT
FOR SOUTHERN DISTRICT OF OHIO
WESTERN DIVISION

IN THE MATTER OF THE SEARCH OF:

[REDACTED]

Case No. 3:21MJ358

**AFFIDAVIT IN SUPPORT OF AN
APPLICATION UNDER RULE 41 FOR A
WARRANT TO SEARCH AND SEIZE**

I, Robert McGuire, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a warrant to search the premises known as [REDACTED] (the “SUBJECT PREMISES”) further described in Attachment A, for the things described in Attachment B.

2. I am a Special Agent with the Federal Bureau of Investigation (“FBI”) and have been in this position since 2005. During my tenure with the FBI, I have worked on investigations involving public corruption and fraud. While at the FBI Academy, I received training on various types of fraud offenses and how such crimes are perpetrated. I have also received training on how criminals use technology to perpetrate crimes. These trainings have included specific guidance and instruction on how criminals use and manipulate technology and how criminals can exploit vulnerabilities in computer systems. Prior to joining the FBI, I received my Master of Business Administration degree with a concentration in Management Information Systems. In my 17 years with the FBI, I have worked on at least five investigations in which I was required to seize and

compile electronic data, review electronic communications, or otherwise handle evidence extracted from technological devices.

3. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses.

4. This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

PROBABLE CAUSE

5. The FBI is currently investigating [REDACTED] for alleged wire fraud, in violation of 18 U.S.C. § 1343. Based on the investigation to date, it appears that [REDACTED] is defrauding an 86-year-old man (“Individual 1”) into providing funds for fictitious investments in, among other things, rubber and Bitcoin mining.² Rather than investing these funds on behalf of Individual 1, [REDACTED] seems to be spending them as he chooses, including on after-market accessories for his cars, down payments on cars, expensive clothing, and expensive shoes. Given the facts alleged in this Affidavit, I respectfully submit that there is probable cause to believe that evidence and instrumentalities of this alleged wire fraud scheme will be found in the SUBJECT PREMISES, including among other things, electronic records, cellular telephones, and computers.

¹ The individuals who provided information about [REDACTED] did not necessarily use his full name.

² Bitcoin is a cryptocurrency that is “mined” using computers.

Information Received from Individual 1's Family Members

6. As part of its investigation, the FBI has received information from Individual 1's family, including his two adult sons ("Individual 2" and "Individual 3") and two adult daughters ("Individual 4" and "Individual 5"). In interviews and communications occurring from July 23, 2021 to present, one or more of the family members conveyed the following information to the FBI, in substance and in part:

- a. Individual 1 is the founder and majority (51%) owner of an engineering and surveying business located in the Southern District of Ohio ("Company A"). The remaining ownership of Company A is split between Individual 1's sons, Individual 2 and Individual 3, who are the COO and Director of Sales and Marketing, respectively. Individual 4 acts as a personal assistant to Individual 1. Individual 5 manages the website for the business.
- b. Approximately a decade ago, Individual 1 was introduced to [REDACTED] through a friend. The friend informed Individual 1 that [REDACTED] could do carpentry work. Not long after, [REDACTED] began offering to help Individual 1 in purchasing vehicles for Company A and to assist Individual 1 in other investments.
- c. Over the last 10 years or so, Individual 1 has given [REDACTED] money for purported investments in, among other things, rubber, cars, real estate, and Bitcoin mining. Individual 1's family estimates that he has borrowed around two million dollars from Company A to give to [REDACTED]. In the past two years, Individual 1 has

given [REDACTED] money more frequently and in higher amounts than in previous years.

- d. At some point, Individual 1 gave a check to [REDACTED] to use for paying real estate taxes on some land that Individual 1 owned. [REDACTED] neglected to pay the taxes and as a result, the land was forfeited and sold at auction.
- e. [REDACTED] was supposed to procure 8 trucks for Company A. Only 4 were received, and those 4 that were procured did not fit the description of what [REDACTED] was expected to get.
- f. The purported rubber investment started approximately six years ago. [REDACTED] claims to have a warehouse full of rubber purchased by Individual 1, with the rubber as an investment vehicle to sell in the future. Individual 1 told Individual 4 that the rubber was stored in a warehouse in Columbus but was moved to Tennessee. [REDACTED] told this to Individual 1 after being asked by Individual 1 to see the rubber.
- g. Approximately two years ago, Individual 1 acquired some Bitcoin. About a year later, Individual 1 told [REDACTED] about his Bitcoin, and [REDACTED] offered to purchase computers to mine more.
- h. Over time, [REDACTED] purports that he has an individual named [REDACTED], who is assisting with these investments. [REDACTED] has said that [REDACTED] assists with mining

Bitcoin and purchasing computers that mine Bitcoin. Individual 1 has never met [REDACTED] in person.

- i. In around 2018, Individual 1's family received anonymous correspondence from an informant claiming, in substance, that [REDACTED] was scamming Individual 1.
- j. Individual 1's family has spoken repeatedly with Individual 1 about his dealings with [REDACTED] Individual 1 trusts [REDACTED]. As conveyed to the FBI in an email from Individual 2 on or about August 26, 2021, Individual 2 spoke to Individual 1. Among other things, Individual 1 relayed the following information concerning the conversation:

- i. Individual 2 asked Individual 1 about money that had disappeared from Company A during the winter/early spring (which Individual 2 placed at around \$500,000 to \$750,000). Individual 1 said that he "borrowed the money and rolled most of it into the rubber account." Individual 1 said that there was an investor.
- ii. Individual 2 asked Individual 1 about "the 8-10 trailers [Individual 1] bought through borrowing the company money this year." Individual 1 said that "he bought them to roll them into bitcoin."
- iii. Individual 2 asked Individual 1 why he had given [REDACTED] around \$80,000.00 in the last three to four months, and Individual 1 said that [REDACTED] "takes the money and puts it toward the investment deal etc. as

[Individual 1] tells him to.” Individual 1 said that [REDACTED] only “does what [Individual 1] tells him to do with the money mostly toward the deal.” Individual 1 said that he “knows where all the money is going” and that “it is all recorded in his checkbook or on his iPhone.”

iv. Individual 1 said that the [REDACTED] was “about to die.” After Individual 2 remarked that “that has happened at least three time in the past 10 years,” Individual 1 laughed and said that it had. Individual 1 said that he had talked with [REDACTED] on the phone and met [REDACTED]. Individual 1 would not answer if he had met [REDACTED] in person.

k. In one of the text message exchanges between Individual 1 and [REDACTED], Individual 1 asks for the bitcoin so that he can pay back the company for all the money he has invested and so his sons will back off because they have seen a lot of money leave the company for these investments and no money or bitcoin has ever been given back.

l. No one in Individual 1’s family has seen anything indicating that [REDACTED] has actually invested Individual 1’s money into rubber or Bitcoin.

7. Individual 1’s family provided the FBI with a copy of the anonymous correspondence alleging that Individual 1 was being “conned and robbed out of every dime he has” by [REDACTED] and [REDACTED] associates. The correspondence, which is undated, has been

attached to this Affidavit as Exhibit 1 and is incorporated herein by reference.³ A portion of the correspondence appears to be addressed to Individual 1, and another portion to his family. The correspondence states the following, in substance and in part:

- a. The author is very familiar within Individual 1, his business, and his associates.
- b. [REDACTED] and others are conning Individual 1 out of hundreds of thousands of dollars. The others include [REDACTED].
- c. [REDACTED] and others have posed as potential investors or buyers. [REDACTED] has texted Individual 1 using a prepaid phone with a fake number while pretending to be investors. Others have spoken with Individual 1 over the phone.

8. Individual 4 provided the FBI with images of Individual 1's checkbook ledger for his personal account at Huntington Bank. The ledger appears to document checks that have been written against Individual 1's account during the period of around April 6, 2021 through June 21, 2021, and it appears to include a number, date, transaction description, and amount for most, if not all, checks written during that time period. Notably, the ledger contains several entries that reference [REDACTED] (presumably [REDACTED]) and one or more of the following: "rubber," [REDACTED] variations of "Bitcoin," and terms related to Bitcoin (such as "mining"). Certain of these entries

³ Only the text of the correspondence itself has been included as Exhibit 1. The correspondence refers to a "packet" and "evidence." In addition to the written portion of the correspondence, Individual 1's family has sent the FBI copies of what appears to be a search for [REDACTED] name in a court records database and images from what appear to be Facebook pages related to individuals mentioned in the correspondence. Apparent references of the names of the family members and one other individual are redacted.

appear to contain the term “trailer.” In total, it appears that, during the time period covered by the images of the ledger, Individual 1 has written approximately 20 checks related to rubber or Bitcoin for a total of approximately \$70,500.

9. Individual 1 and [REDACTED] communicate over the phone, overwhelmingly through calls, but also through text messages. Based on interviews of the family and on the images of Individual 1’s phone, Individual 1’s cell phone is an iPhone. Additionally, in the text message exchanges between Individual 1 and [REDACTED], all of the messages sent from Individual 1 are blue. This indicates that both parties are communicating over iMessage, an Apple messaging service only available for use on iOS devices. The content of these messages includes [REDACTED] asking Individual 1 to call him or Individual 1 asking [REDACTED] to call him.

10. Additionally, at various times from August 31, 2021, through September 17, 2021, Individual 2 provided the FBI with images of what Individual 1’s iPhone. The images show what appear to be text messages between (a) Individual 1 and [REDACTED] and (b) Individual 1 and [REDACTED]

- a. In messages believed to be from August 3, 2021,⁴ [REDACTED] request money for assistance that is needed due to [REDACTED] health.

⁴ The year of the messages is not shown in the images described in the subparagraph. Based on the date the images were sent to the FBI, it is believed that the messages were from August 2021. Similarly, with respect to the messages described in the two following subparagraphs, those exchanges, although undated in the images, are believed to have occurred in September 2021 based on when they were sent to the FBI.

- b. In one of the text message exchanges believed to be from September 2021 between Individual 1 and [REDACTED], Individual 1 asks for the Bitcoin so that he can pay back the company for all the money he has invested and so that his sons will back off because they have seen a lot of money leave the company for these investments and no money or Bitcoin has ever been given back.
- c. Individual 1 further tells [REDACTED]: “From the boys standpoint they have seen a lot of money go out of the company and they think [REDACTED] is stealing it I cannot convince him that he hasn’t until I show them some of the money back because I’ve sold 362 or get the bit coins in in my possession.” This affiant understands 362 is a building owned, or previously owned, by Individual 1, based on information provided by Individual 1.

Interview of [REDACTED]

11. On or about August 16, 2021, the FBI met with and interviewed an individual (“Individual 6”) who identified herself as [REDACTED], who was identified through the anonymous letter. During the interview, Individual 6 provided the following information, in substance and in part:

- a. Sometime in approximately 2018, Individual 6 lived with [REDACTED], her then-boyfriend, at the SUBJECT PREMISES. Individual 6 dated [REDACTED] on and off for about a year. She has not talked to him much in the last couple years.
- b. According to Individual 6, [REDACTED] used two cell phones.

- c. She communicated with [REDACTED] on the cell phone with the number [REDACTED]. [REDACTED] Individual 6 did not remember [REDACTED] other cell phone number. [REDACTED] kept a pre-paid phone in his drawer, but Individual 6 did not know anything about that phone.
- d. [REDACTED] told Individual 6 that he had a car dealer's license and would use it to buy cars at the auction. [REDACTED] got into an argument with an employee at the auction and was no longer allowed to attend. An old man who wore gold chains would go to the auction for [REDACTED].
- e. [REDACTED] owned a lot of cars and often had them worked on at Xtreme Autosports in Dayton. He liked to jack up trucks that he bought, and Xtreme Autosports would do the work. [REDACTED] was friends with the people who worked there.
- f. [REDACTED] has a friend named [REDACTED] whom [REDACTED] considers to be his brother. [REDACTED] was previously married to [REDACTED], who has a sister named [REDACTED]. [REDACTED] is married to [REDACTED]. Individual 6 did not know who [REDACTED] were.
- g. [REDACTED] talked often about a man he referred to as "Old Man [Name]"⁵ "Grandpa," or "Uncle." Individual 6 often heard [REDACTED] speak on the phone

⁵ Individual 6 used a name that is a nickname for Individual 1's first name. Accordingly, Individual 1 is used to refer to the person with whom [REDACTED] was speaking.

with Individual 1. [REDACTED] would tell Individual 1 that [REDACTED] was picking up cars and needed money. Individual 1 would then put a check in the mailbox for [REDACTED]. Individual 6 knew that [REDACTED] was lying to Individual 1, and that [REDACTED] was just getting the money for his own use. According to Individual 6, [REDACTED] would make up stories to get money from Individual 1. [REDACTED] told Individual 1 that he had been in meetings with people and discussed buying cars and therefore needed money from Individual 1. [REDACTED] may have told Individual 1 that these people were investors. Individual 6 rode with [REDACTED] to pick up the checks. They picked up checks almost every day. Individual 6 was not allowed to pick up the checks; only [REDACTED] and [REDACTED] were allowed to pick up the checks.

- h. [REDACTED] wasted the money he had on shoes and clothes. He had stacks of Air Jordan shoes, and he bought clothes for his friends and Individual 6.
- i. [REDACTED] always bought things with credit cards. Individual 6 was not sure whose name was on the cards. She thought it was [REDACTED] name, but he did not allow her to see the cards.
- j. [REDACTED] made Individual 6 think she was crazy and on drugs. He convinced her to check into a drug rehabilitation facility. When facility personnel evaluated her, they questioned why she was there because she was not taking drugs. Individual 6 left the facility.

- k. [REDACTED] did not like Facebook and never wanted to have his picture posted on Facebook or any other social media.

Information from [REDACTED]

12. On or about August 13, 2021, the FBI visited [REDACTED] an automotive shop in Moraine, Ohio to serve a subpoena for records of purchases associated with Individual 1 or [REDACTED]. In reviewing records received in response to the subpoena, the FBI has learned that, during roughly the first five months of 2021, [REDACTED] appears to have purchased over \$35,000 worth of accessories and labor from [REDACTED].

13. When serving the subpoena on [REDACTED] the FBI interviewed the current owner ("Individual 7") and an employee ("Individual 8"), who provided the following information, in substance and in part:

- a. Individuals 7 and 8 deal with [REDACTED], who brings his vehicles to [REDACTED] to have them modified with after-market parts. Occasionally, [REDACTED] has had vehicle mechanical parts worked on.
- b. Individuals 7 and 8 had not seen [REDACTED] in a couple of months, but prior to that, [REDACTED] was coming in once per week to get work done on a car or truck. Each vehicle has been different.
- c. [REDACTED] recently brought in a Jeep to have it lifted. Individual 7 suspected [REDACTED] would not keep the vehicle once [REDACTED] completed the work on it and

accused [REDACTED] of selling his cars quickly after buying them. [REDACTED] sold the vehicle shortly thereafter.

- d. When paying for work performed by [REDACTED], [REDACTED] hands the phone to Individual 7 or Individual 8. On the phone is a man with the same first name as Individual 1 whom [REDACTED] calls his [REDACTED]. [REDACTED] says that [REDACTED] is rich from owning companies. The credit card used is an American Express card.

Interviews of Individuals Who Purchased Trailers from [REDACTED]

14. The FBI interviewed two individuals (“Individual 9” and “Individual 10”) who claim to have purchased trailers from [REDACTED]

- a. On or about August 20, 2021, the FBI interviewed Individual 9, who identified himself as the former owner of [REDACTED]. Individual 9 provided the following information, in substance and in part:
 - i. Individual 9 sold [REDACTED] and now lives outside of Ohio.
 - ii. Individual 9 bought a trailer from [REDACTED] y. In January 2021, [REDACTED] asked Individual 9 to sell it back. Individual 9 understood that [REDACTED] originally used the trailer for the rehab work that [REDACTED] did for his job. [REDACTED] never mentioned anything to Individual 9 about hauling rubber with the trailer.

- iii. Individual 9 also bought a 2008 Chevy Silverado from [REDACTED], which [REDACTED] asked Individual 9 to sell back to him. [REDACTED] told Individual 9 that his grandpa wanted the truck back.
 - iv. [REDACTED] hangs around with someone he referred to as his brother. Individual 9 does not like this person and would not allow him into [REDACTED] if he was with [REDACTED]
- b. On or about August 23, 2021, the FBI interviewed Individual 10, who is friends with [REDACTED]. Individual 10 provided the following information, in substance and in part:
- i. Individual 10 is self-employed and performs work on various things, including golf carts and jet skis. He also builds decks. Individual 10 has his own company.
 - ii. Individual 10 is friends with [REDACTED] but does not trust him based on a lie he told. [REDACTED] asked Individual 10 for money for funeral expenses for a deceased family member. However, Individual 10 found out from someone else that the funeral was fully paid for prior to the death of [REDACTED] family member and that the deceased was cremated.
 - iii. Individual 10 has done work for [REDACTED], and they trade items or labor for payment for the work.

- iv. [REDACTED] works for M&M Construction. [REDACTED] and Individual 10 once performed work on the same house. The work performed by [REDACTED] was messed up.
- v. [REDACTED] has approximately 150 pairs of jeans that cost approximately \$200 per pair. [REDACTED] also has a closet full of Nike shoes and stacks of guns in his house.
- vi. Individual 10 owns five trailers and bought at least some of them from [REDACTED]. According to Individual 10, [REDACTED] got good deals on trailers, which were originally purchased from the Rodeo Shop.
- vii. [REDACTED] has not mentioned anything to Individual 10 about possessing a car-dealer license, nor has [REDACTED] mentioned anything about hauling rubber or mining Bitcoin. [REDACTED] has, however, asked Individual 10 about Bitcoin. [REDACTED] has never mentioned anyone named [REDACTED].

Information from [REDACTED]

15. On or about July 30, 2021, the FBI interviewed three employees of [REDACTED] a car dealership located in the Southern District of Ohio. The employees included the general manager, a salesman, and a buyer. During the interview, the employees provided the following information, in substance and in part:

- a. [REDACTED] changes cars often and buys them from this dealer. He has poor credit, and it is difficult to get his deals done as a result. [REDACTED] includes a down payment when he purchases cars.
- b. [REDACTED] trades cars every couple of months and once traded in a car after only two weeks of ownership. He refers to his rich [REDACTED] during the purchases. [REDACTED] called his rich [REDACTED] for a \$10,000 down payment.

16. On or about August 16, 2021, one of the employees at [REDACTED] sent the FBI “DEAL RECAP” documents that appear to relate to 16 transactions between the dealership and [REDACTED]. The transactions occurred during the approximate time period of November 29, 2018 through July 15, 2021. The documents all list [REDACTED] name and address (*i.e.*, the address of the SUBJECT PREMISES). In short, the documents appear to show that from 2019 to 2021, [REDACTED] purchased 16 cars from [REDACTED].

Individual 1’s Credit Cards

17. On or about a subpoena was served on American Express seeking records related to Individual 1’s credit card (ending in 5017) for the period January 1, 2017 to the present. A review of Individual 1’s credit card statements received in response to the subpoena has revealed that, during the period from January 1, 2017 to the present, Individual 1’s credit card account has incurred charges of over \$190,000 at Beau Townsend Ford/Nissan/Lincoln, over \$100,000 at [REDACTED], and over \$80,000 at Xtreme Autosports.

██████████ Key Bank Account

18. On or about August 4th, 2021, a subpoena was served on Key Bank seeking records related to any of ██████████ bank accounts, loans, and/or credit cards from 2017 to the present.

19. In reviewing the records, it appears that, from November 2019 to August 2021, there were around 153 checks from Individual 1 or an LLC owned by Individual 1 (“Company B”) deposited into ██████████ bank account. Most of these checks reference “loan” in the memo line. Other checks reference trailers, vehicles, and real estate. The checks total over \$550,000.

20. In reviewing the April 2021 bank statement, it appears that:

a. A total of around \$61,214.62 was deposited into ██████████ Key Bank account. Over \$38,000 of that is from checks from Individual 1 and/or Company B.

i. Based on the check numbers, some of these checks appear to correspond to entries in Individual 1’s checkbook ledger for rubber.

b. Around \$31,089.10 in total was withdrawn, spent, or drawn from checks from ██████████ account.

c. Over \$8,000 in cash was withdrawn from ATMs and Bank withdrawals.

d. No purchases in April seem to be towards Bitcoin or rubber investments.

21. In reviewing the May 2021 bank statement, it appears that:

a. A total of around \$26,188.23 was deposited into ██████████ Key Bank account. Over \$26,000 of that is from checks from Individual 1 and/or Company B.

- i. Based on the check numbers, some of these checks appear to correspond to entries in Individual 1's checkbook ledger for rubber and Bitcoin.
 - b. Around \$33,231.89 in total was withdrawn, spent, or drawn from checks from [REDACTED] account.
 - c. Over \$13,500 in cash was withdrawn from ATMs and Bank withdrawals.
 - d. No purchases in May seem to be towards Bitcoin or rubber investments.
22. In reviewing the June 2021 bank statement, it appears that:
- a. A total of around \$30,648.46 was deposited into [REDACTED] Key Bank account. Approximately \$27,000 of that is from checks from Individual 1 and/or Company B.
 - i. Based on the check numbers, some of these checks appear to correspond to entries in Individual 1's checkbook ledger for rubber and Bitcoin.
 - b. Around \$38,535.40 in total was withdrawn, spent, or drawn from checks from the account.
 - c. Over \$6,800 in cash was withdrawn from ATMs and Bank withdrawals.
 - d. No purchases in June seem to be towards Bitcoin or rubber investments.

Information from Ohio Department of Taxation

23. On or about August 31, 2021, a subpoena was served on the Ohio Department of Taxation for tax records filed in the state of Ohio in years 2017-2021. A review of the letter and

records provided by the Ohio Department of Taxation in response to the subpoena disclosed the following information, in substance and in part:

- a. As of September 9, 2021, [REDACTED] address was listed in the records as [REDACTED] (*i.e.*, the address of the SUBJECT PREMISES).
- b. [REDACTED] did not file Ohio tax returns related to personal income for the years 2017, 2019, and 2020. Similarly, [REDACTED] did not file Ohio tax returns related to business taxes for the years 2017 through 2021.
- c. [REDACTED] filed an Ohio tax return related to personal income for the year 2018. According to a summary of his 2018 return, [REDACTED] reported a federal adjusted gross income of -\$2,584, an Ohio adjusted gross income of -\$5,861, and no taxable business income. The 2018 return summary also indicated that [REDACTED] reported that he owed no Ohio income tax.

Search for Prior Criminal History

24. On or about September 16, 2021, the FBI conducted a search for criminal history records related to [REDACTED]. This search revealed [REDACTED] does not have any arrests or convictions for criminal acts.

25. On or about September 27, 2021, the FBI reviewed online records from the Miami County (Ohio) Court of Common Pleas. The online records indicate that [REDACTED] was a

defendant in two criminal forgery cases from 2004. No indicted charge or disposition is listed in the online records for either case, and both cases appear to be closed.

Search of Accurint

26. On or about September 27th, 2021 the FBI searched records to confirm that [REDACTED] lives at the SUBJECT PREMISES.

Surveillance of the SUBJECT PREMISES

27. On or about August 10, 2021, the FBI conducted surveillance of the SUBJECT PREMISES and observed [REDACTED] in the driveway and departing in a White Chevrolet Silverado. On or about September 28, 2021, the FBI also conducted surveillance of the SUBJECT PREMISES; the same Silverado was located in front of the SUBJECT PREMISES and a 2017 Ford F-150 registered to [REDACTED] was located in the driveway.

Training and Experience Concerning Records of Transactions and Financial Fraud

28. Based on my training and experience, I am aware that records of financial and bank transactions are increasingly sent and received electronically and found on cellular telephones and computers. Cellular telephones, including iPhones, can be backed up on computers or other devices, allowing for the transfer of photographs and other records that may contained evidence of fraud or the fruits of fraud. Cellular telephones, laptops, home computers, and hard drives can store pictures, financial documents, or correspondence, which could document the spending habits and source of income of the user. Moreover, a cellular telephone, laptop, or computer could contain a history of the user's Internet searches, which could lead to evidence concerning how a

scheme is perpetrated. Additionally, because Bitcoin is “mined” on computers and is traded electronically, computers may contain evidence in Bitcoin-related schemes, including the absence of any indication that the computers are being used for purposes of mining Bitcoin. People sometimes leave or store cellular telephones or other devices in their vehicles. Records of who owns or uses the vehicles are often stored inside the vehicles.

TECHNICAL TERMS

29. Based on my training and experience, I use the following technical terms to convey the following meanings:

- a. IP Address: The Internet Protocol address (or simply “IP address”) is a unique numeric address used by computers on the Internet. An IP address looks like a series of four numbers, each in the range 0-255, separated by periods (e.g., [REDACTED]). Every computer attached to the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.
- b. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections

between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

- c. Storage medium: A storage medium is any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

COMPUTERS, ELECTRONIC STORAGE, AND FORENSIC ANALYSIS

30. As described above and in Attachment B, this application seeks permission to search for records that might be found on the SUBJECT PREMISES, in whatever form they are found. One form in which the records might be found is data stored on a computer's hard drive or other storage media. Thus, the warrant applied for would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

31. *Probable cause.* I submit that if a computer or storage medium is found on the SUBJECT PREMISES, there is probable cause to believe those records will be stored on that computer or storage medium, for at least the following reasons:

- a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later

using forensic tools. This is so because when a person “deletes” a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

- b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer’s operating system may also keep a record of deleted data in a “swap” or “recovery” file.
- c. Wholly apart from user-generated files, computer storage media—in particular, computers’ internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory “swap” or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.
- d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or “cache.”

32. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes

described on the warrant, but also for forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any storage medium in the SUBJECT PREMISES because:

- a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.
- b. As explained herein, information stored within a computer and other electronic storage media may provide crucial evidence of the “who, what, why, when, where, and how” of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent

from further suspicion. In my training and experience, information stored within a computer or storage media (e.g., registry information, communications, images and movies, transactional information, records of session times and durations, internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculcating or exculpating the computer owner. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, as described herein, computers typically contain information that log: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and

have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (e.g., a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculcate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user's state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (e.g., internet searches indicating criminal planning), or consciousness of guilt (e.g., running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

- c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.
- d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely

reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

- e. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

33. *Necessity of seizing or copying entire computers or storage media.* In most cases, a thorough search of a premises for information that might be stored on storage media often requires the seizure of the physical storage media and later off-site review consistent with the warrant. In lieu of removing storage media from the premises, it is sometimes possible to make an image copy of storage media. Generally speaking, imaging is the taking of a complete electronic picture of the computer's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

- a. The time required for an examination. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine storage media to obtain evidence. Storage media can store a large volume of information. Reviewing that information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.
- b. Technical requirements. Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on the premises. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.

- c. Variety of forms of electronic media. Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

34. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, or otherwise copying storage media that reasonably appear to contain some or all of the evidence described in the warrant, and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

35. Because people share the SUBJECT PREMISES as a residence, it is possible that the SUBJECT PREMISES will contain storage media that are predominantly used, and perhaps owned, by persons who are not suspected of a crime. If it is nonetheless determined that that it is possible that the things described in this warrant could be found on any of those computers or storage media, the warrant applied for would permit the seizure and review of those items as well.

CONCLUSION

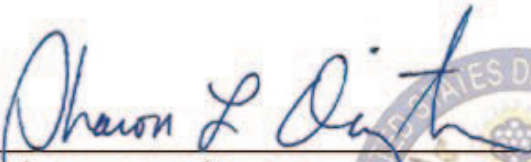
36. I submit that this affidavit supports probable cause for a warrant to search the SUBJECT PREMISES described in Attachment A and seize the items described in Attachment B.

Respectfully submitted,



Robert McGuire
Special Agent
Federal Bureau of Investigation

Subscribed and sworn to before me
on September 28, 2021:



Sharon L. Ovington
United States Magistrate Judge



EXHIBIT 1

Dear [REDACTED] Family,

I am writing you this letter and forwarding you a copy of the packet that I mailed to Mr [REDACTED]. I have tried to help make this process for him and you a little easier by including more than enough evidence of the fact he is being conned and robbed out of every dime he has and has worked hard for by a few mistakes of society, drug abusers, users, conmen, losers, manipulators. None of these people have ever worked, all have drug abuse problems and all have one thing in common, they are taking [REDACTED] and [REDACTED] for everything they can. When [REDACTED] and [REDACTED] were made aware of the money [REDACTED] was conning [REDACTED] out of and [REDACTED] found out he now has [REDACTED] write him checks only from him and [REDACTED]'s personal checking and transfer the money in from the business account, [REDACTED] and [REDACTED] and the others then go to Huntington bank right by [REDACTED] and [REDACTED]'s home to cash the checks.

Look at all the pictures enclosed, these are pictures of cars [REDACTED] has bought with [REDACTED]'s money, motorcycles, clothes, shoes, dinners, new phones, and I have even included the Xtreme autosports on Main street in Dayton has helped him con from [REDACTED] and [REDACTED] newest car that [REDACTED] will be paying for without knowledge. As you will see in the pictures, [REDACTED] will be called soon by Xtreme to tell him they have done work on a car tyhat he owns, [REDACTED] owns no cars, these are lies [REDACTED] and Xtreme hacve told him, when in reality that call will be for all the customizing [REDACTED] is having done on a Chrysler 300 for him and his heroin addict girlfriend.

Please just look in to all the evidence and things I am sending you, you will see [REDACTED] and his associates are cleaning out [REDACTED] and [REDACTED]'s accounts including running up well over \$100,000 on [REDACTED] credit cards.

[REDACTED]
[REDACTED]
[REDACTED] on facebook

[REDACTED] on facebook

[REDACTED] on facebook

[REDACTED] all profiles
on facebook

Dear [REDACTED],

You do not know me but I am very familiar with you, your business, and associates. I am writing this letter in regards to [REDACTED] and the others involved.

You are very familiar with [REDACTED] and well aware of the many 100's of thousands of dollars you have given him over many years, you should also be familiar with [REDACTED] who you have also written thousands of dollars of checks too which is [REDACTED] very good friend that has helped [REDACTED] Con you and has told you many lies to embezzle a very large um of money from you. [REDACTED] is no business man, he has never made any trips out of town for you, he has never picked up any cars for you. As you should know you do not own any cars, those too are lies.

[REDACTED] is better known as [REDACTED] is a convict and a drug addict as well as his girl friend [REDACTED] they have also helped [REDACTED] con you for your money pretending to be people on the phone that were interested in your properties for sale. You should know none of these people including [REDACTED] have any money to buy anything from you. They are using your money for shopping sprees and drugs.

[REDACTED] has embezzled thousands of dollars from you and makes jokes stating that you are old and you cannot take it with you and that your spoiled ass kids and grandkids dont deserve it. [REDACTED] has made multiple statements about as long as your stupid enough to believe him that he will continue to take every penny you have. [REDACTED] laughs and said, "I have gotten close to probably a million from his old ass in the last 6 or 7 years." [REDACTED] also laughs and states how he made you believe your sons([REDACTED]) were liars about him because he knows that they realize he is ripping you off. [REDACTED] also sold all of the gold coins that you thought were being given to a possible property buyer, this was also lies. There are NO potential investors. When you believe you are texting these potential buyers these are actually steven using a prepaid phone and fake number and pretending to be the investors. Dont you

understand why you have never met these people? There is and never was a [REDACTED] a [REDACTED] or any other potential buyers. LIES LIES LIES.. [REDACTED] has also made statements about your wifes illness and that the money wouldnt help her anyways. [REDACTED] has manipulated you and made a fool out of you, your family, and your business. The Mustang that you believe you have put so much money into is actually in a storage unit on 4 flats, ripped top, and dont even start, this unit is located at Korrekt storage on route 35 in Dayton and is set to be auctioned off this week for nonpayment, unit is in [REDACTED] name. Also all of the credit card transactions you are allowing [REDACTED] to do by phone with Xtreme auto sports on Main street in Dayton are for customizing his vehicles from 5000.00 rims and 2000.00 tires to music systems and lifts for his truck, none of these transactions are for anything you own or for any potential buyers.

This is just some of the information I know, however, I did not want to disclose all of the information as you have been told this many times before and have not believed anyone including your own children. A man of your intelligence should have known better. [REDACTED] and his associates are bums, drug addicts, conmen, and will bust hell wide open for the things they have done to so many including your family. You childrne love you and had your best interest at heart and you shunned them and challenged there intelligence for a man who would not care if you died tomorrow accept that he would no longer get any more money from you as he has stated this from his own mouth. WAKE UP Mr [REDACTED] before you have nothing left. So to help I am enclosing pictures of the luxury [REDACTED] and everyone else is using your money for. This ranges from 400.00 dinners, 200.00 pairs of jeans, motorcycles, trucks, tattoos, drugs, etc. Also i'll include arrest records for the people you have been giving your life savings to.

If you confront [REDACTED] about any of this he will lie to you and try to get out of it, so instead why dont you just take a little time to read thru this and do some investigation yourself. Everyone sees and knows what he is doing to you but you. Please listen before it is too late. Look at the pics, look at the records, look at the facebooks I have enclosed photos of. Just keep an open mind and ask yourself, What if this is all true, youve lost thousands and thousands that you were your entire life for. [REDACTED] has never actually worked in his life.

One more piece of information, you are not the only one he has taken from, contact [REDACTED] of M&M construction and ask him about money he is owed for things he thought he was purchasing that did not exisat either.

I am also forwarding these pictures to your children and to the police department so they will all know what this CONMAN has done and taken from you.

I AM TRYING TO HELP YOU< ITS UP TO YOU TO TAKE IT [REDACTED] !!